Евстратенко Елена Сергеевна
аспирант
Селифанов Валентин Валерьевич
старший преподаватель
Старикова Алёна Алексеевна
студентка
ФГБОУ ВО «Новосибирский государственный университет экономики и управления «НИНХ»
г. Новосибирск, Новосибирская область

ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С УЧЕТОМ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация*: в данной работе рассмотрены государственные информационные системы, которые создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами. В таких системах обрабатывается как общедоступная информация, так и информация ограниченного доступа.*

Ключевые слова*: информация, защита информации, обработка информации, риски, государственные информационные системы, управление рисками.*

На сегодняшний день в Российской Федерации приняты нормативные правовые акты, регламентирующие необходимость защиты информации, содержащейся в государственной информационной системе. Федеральный закон (далее – ФЗ) №149 от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» обязывает владельца информации и оператора информационной системы, обеспечивать защиту информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий (ст.14 п.9) путем принятия правовых, организационных и технических мер, направленных на соблюдение конфиденциальности информации ограниченного доступа и реализацию

права на доступ к общедоступной информации (ст. 16) [1]. В соответствии с ФЗ №149 утверждены требования о защите информации Приказом ФСТЭК России от 11 февраля 2013 г. №17, которые являются обязательными к исполнению [2].

Построение системы защиты информации информационной системы (далее – СЗИ ИС) начинается с определения требований к ней с учетом ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Указанные требования определяются обладателем информации или заказчиком в зависимости от класса защищенности информационной системы и выявленных угроз безопасности информации, включенных в модель угроз [2].

Требования в зависимости от выявленных угроз безопасности информации ГОСТ Р 51583–2014 рекомендует формировать, основываясь на оценке рисков информационной безопасности, согласно ГОСТ Р ИСО/МЭК 27005 – 2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [8].

После того как были сформированы требования к СЗИ ИС необходимо выбрать меры реализации требований к СЗИ ИС. В Приказе ФСТЭК России №17 в приложении №2 представлены базовые наборы мер защиты информации для соответствующих классов защищенности информационных систем. При оценке рисков могут быть выявлены угрозы безопасности информации, блокирование которых мерами защиты, приведенными в Приказе ФСТЭК России №17, невозможно, в таком случае могут применятся иные меры нейтрализации угроз [2].

В ходе эксплуатации информационной системы перед оператором встает задача анализа изменения угроз и принятия мер их нейтрализации. Приказ ФСТЭК России №17 содержит требования по анализу инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий в ходе эксплуатации информационной системы, и принятию мер по устранению инцидентов (пункт 18.2) [2], однако ни указанный документ, ни методический документ «Меры защиты информации в государственных информационных системах» [9] не содержат рекомендаций по решению данной задачи.

Анализ изменения угроз заключается в периодическом пересмотре модели угроз и выявления вновь актуальных угроз, другими словами в оценке рисков информационной безопасности. Для оценки рисков информационной безопасности можно применить международный стандарт семейства стандартов 2700х ГОСТ Р ИСО/МЭК 27005 – 2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», рекомендованный ГОСТ Р 51583 при формировании требований к СЗИ ИС.

ГОСТ Р ИСО/МЭК 27005 определяет процесс управления рисками, как циклический процесс, требующий периодической переоценки факторов риска и периодического мониторинга новых активов, угроз, уязвимостей, модификации ценности активов, вероятности реализации угроз и инцидентов [6].

В международной практике помимо стандарта ГОСТ Р ИСО/МЭК 27005 для управления рисками ИБ существует ГОСТ Р ИСО 31000–2010 «Менеджмент риска. Принципы и руководство» и к нему дополнение ГОСТ Р ИСО/МЭК 31010–2011 «Менеджмент риска. Методы оценки риска», который содержит рекомендации по выбору и применению методов оценки риска [7].

После оценки рисков оператором информационной системы должно быть принято решение о принятии мер и средств для снижения, сохранения, предотвращения или переоценки риска на основании определенных критериев оценки риска, его влияния и принятия риска [6].

Выбор мер и средств защиты информации может осуществляется как из состава мер, представленных в Приказе ФСТЭК России №17, так и из иных источников. В качестве иного источника можно представить ГОСТ Р ИСО/МЭК 27002 – 2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», содержащий требования, меры и средства защиты информации и рекомендации по их реализации [5].

Таким образом, в ходе построения системы защиты информации государственной информационной системы с учетом управления рисками информационной безопасности могут применятся не только нормативно-правовые акты

Российский Федерации, но и международные стандарты. Так для формирования требований к СЗИ ИС, анализа изменения угроз и принятия мер их нейтрализации применяются ГОСТ Р ИСО/МЭК 27005 – 2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» и ГОСТ Р ИСО/МЭК 27002 – 2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [11].

Применение семейства стандартов 2700х дает возможность организации, использующей данную информационную систему, определить собственный подход к управлению рисками в зависимости от области применения информационной системы, выбрать компенсирующие меры нейтрализации появившихся угроз, а также получить сертификат соответствия системы управления информационной безопасности требованиям стандарта ГОСТ Р ИСО/МЭК 27001 – 2012 «Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования» [4]. Сертификация системы управления информационной безопасности позволяет выработать долговременную стратегию развития системы обеспечения информационной безопасности организации, отвечающую актуальным требованиям, проводить комплексные, эффективные и экономически обоснованные меры по обеспечению информационной безопасности, повысить степень привлекательности организации на внутреннем и внешнем рынках, получить официальный и признаваемый во всем мире сертификат, который будет служить важным показателем надежности организации в глазах клиентов, партнеров, акционеров, аудиторов, государственных и контролирующих органов, и застраховать свои информационные риски на наиболее выгодных условиях[10].

Для демонстрации применения семейства стандартов 2700х при построении системы защиты информации государственной информационной системы в качестве примера возьмем государственную информационную систему, состоящую из пяти рабочих станций, сервера базы данных, сервера приложений и веб-сервера, на котором расположен веб-сайт. Рабочие станции, сервер базы данных

и сервер приложений объединены в локальную сеть при помощи коммутатора, подключенного к веб-серверу. Веб-сервер имеет доступ к сети Интернет посредством маршрутизатора.

На рабочих станциях в качестве операционной системы используется Windows 7 Professional, также на них установлен пакет офисных программ Microsoft Office 2013. В качестве серверной операционной системы используется операционная система Windows Server 2012 R2.

В данной государственной информационной системе обрабатываются персональные данные и служебная информация неограниченного доступа.

Государственная информационная система имеет 3 класс защищенности (3 уровень значимости информации, объектовый масштаб ИС).

При обработке персональных данных в локальной ИС, не имеющей доступ к сети Интернет возможна реализация следующих угроз [3]:

– угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;

– угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций (уничтожение, копирование, перемещение, форматирование носителей информации и т. п.) операционной системы или какой-либо прикладной программы (например, системы управления базами данных), с применением специально созданных для выполнения НСД программ (программ просмотра и модификации реестра, поиска текстов в текстовых файлах и т. п.);

– угрозы внедрения вредоносных программ;

– угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;

– угрозы выявления паролей;

– угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ.

Проанализировав последствия от реализации выше представленных угроз и оценив вероятность реализации данных угроз, руководствуясь ГОСТ Р ИСО/МЭК 27005, были выявлены актуальные угрозы, представленные в таблице 1.

Таблица 1

Актуальные угрозы для ИС

Угроза	Вероятность	Пояснение	Последствия	Пояснения	Заключение
Угрозы, реализуемые в ходе загрузки операционной системы	низкая	Установлен пароль на BIOS и приняты организационный меры по усилению парольной политики	высокие	Нарушение конфиденциальности, целостности и доступности информации	Актуальная
Угрозы, реализуемые после загрузки операционной системы	низкая	Приняты организационные меры по усилению парольной политики и по запрету использования неучтенных съемных носителей	высокие	Нарушение целостности, конфиденциальности и доступности информации	Актуальная
Угрозы внедрения вредоносных программ	высокая	Отсутствие средств антивирусной защиты	высокие	Нарушение конфиденциальности, целостности и доступности информации	Актуальная
Угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации	средняя	Отсутствие средств межсетевого экранирования	низкие	Нарушение конфиденциальности	Неактуальная
Угрозы выявления паролей	низкая	Приняты организационные меры по усилению парольной политики	высокие	Нарушение конфиденциальности, целостности и доступности	Актуальная
Угрозы удаленного запуска приложений	высокая	Отсутствие средств антивирусной защиты	средние	Нарушение конфиденциальности, целостности информации	Актуальная

Угрозы внедрения по сети вредоносных программ	высокая	Отсутствие средств антивирусной защиты	высокие	Нарушение конфиденциальности, целостности и доступности информации	Актуальная

Согласно установленному классу защищенности ИС Приказ ФСТЭК России №17 предлагает базовый набор мер защиты информации. Проанализировав его, можно увидеть, что для нейтрализации выявленных актуальных угроз этот базовый набор мер защиты информации в ИС не нуждается в дополнении и уточнении.

Список литературы

1. Об информации, информационных технологиях и о защите информации: федеральный закон РФ от 27 июля 2006 №149-ФЗ // Собрание законодательства РФ.

2. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ от 11 февраля 2013 №17 утвержден Федеральной Службой по Техническому и Экспортному контролю // Собрание законодательства РФ.

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка): утверждена Федеральной Службой по Техническому и Экспортному контролю России 15 февраля 2008 года // Собрание законодательства РФ.

4. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования. Введен 2006–12–27.

5. ГОСТ Р ИСО/МЭК 27002–2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности Введен 2012–09–24.

6. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Введен 2010–11–30.

7. ГОСТ Р ИСО/МЭК 31010–2011. Менеджмент риска. Методы оценки риска. Введен 2011–12–01.

8. ГОСТ Р 51583–2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен 2014–01–28.

9. Меры защиты информации в государственных информационных системах: методический документ от 11 февраля 2014 утвержден Федеральной Службой по Техническому и Экспортному контролю // Собрание законодательства РФ.

10. Селифанов В.А. Способ моделирования процессов управления техническими средствами и система для его осуществления / В.А. Селифанов, В.В. Селифанов. Патент на изобретение RUS 2331096 08.02.2007

11. Селифанов В.А. Способ оценки эффективности управления техническими средствами и устройство для его осуществления / В.А. Селифанов, В.В. Селифанов. Патент на изобретение RUS 2338243 16.04.2007